Multiple Identity-based Cryptography Algorithm (MICA)

Patel Yashkumar Vijaybhai[1]
[1]M.E. Scholar
[1]Department of Computer Engineering
[1]Gujarat Technological University, Ahmedabad, India

Abstract— Cryptography is the study of methods by which safe and secure communication happens where other parties are involved known as adversaries. More precisely, it involves the analysis of protocols to get rid of these so called adversaries which may cause a loop hole the aspects of information security (Non-repudiation, data confidentiality, authentication, data integrity). Real world applications of cryptography are inevitable and eternal. Some of the areas where cryptography plays a vital role are passwords, E-commerce, ATMs etc. Also the fields like Mathematics, Computer science, Electronics, Electrical Engineering uses the concepts of cryptography. There are many small scale devices present in the market i.e. mobile device which have limited resources such as less battery power, limited processing, less memory. There easily could be a security breach in to such light-weight systems, hence secure cryptographic algorithm should be developed to provide the security for data.

Key words: Cryptography, Symmetric-key, Asymmetric-key, Identity-based, Security, Mobile, Sensor, Wireless, GSM, MICA

I. INTRODUCTION

Prior to the present generation, cryptography was just another form of encryption. It just had the techniques of changing the data to unreadable format. This is more often done with help of some encryption algorithms. [1]

Cryptography in the current generation took a major turnaround from its previous era. It is more influenced by mathematical concepts and Computer science practices. The reason behind this being, the mathematical theory applied to cryptography, which makes it difficult for the adversaries to break through. There are various cryptographic algorithms used which in turn uses various mathematical techniques. [2]

A. Symmetric-Key Cryptography

Symmetric key cryptography deals with the encryption where the receiver and sender uses a common key for encryption of plain text and decryption of cipher text. In real time, the key is an "open secret" and is shared between the parties. Here the main disadvantage is so called 'secret key', which actually is being disclosed. And the other disadvantage is that, by knowing the only 'secret key' communication link can be breached.

Symmetric key cryptography was the only method of encryption back in the past generation. These are implemented as stream ciphers and sometimes block ciphers. [3]

B. Public-Key Cryptography

Public key cryptography is the mechanism where there is no need of maintaining the public key secretly and can be disclosed. Although public key can be disclosed, its paired private key must be kept secret. For stricter security increase in the number of members in the network must be met by increase in the number of keys and also by more complex algorithm. So public key cryptography is not an apt solution in the situation where communication between sensors needs to be secure. [4]

Apparently, in case of secured communication between sensors the above mentioned encryption techniques becomes an overhead in terms of processing, algorithm selection, memory and battery power consumption. [5]

II. MULTIPLE IDENTITY-BASED CRYPTOGRAPHY ALGORITHM (MICA)

Multiple Identity based cryptography process best fits in the situations where multiple unique identities can be used. The whole process is divided into two message format:

1) Join Message
2) Data Message

Why two types of message format is required?

In MICA private or public key cryptosystems are not used. The only way to achieve non-repudiation, data confidentiality, authentication and data integrity in MICA is by segregating message into two message formats i.e. join message and data message.

Join message is used for registration of the sensor and data message is used for transferring payload.

A fitting example for practical use of this algorithm is a system which needs to measure the level, velocity, temperature of water using ultrasonic sensor and needs to send this data with the help of GSM module to the centralize server. Here we can use Sensor Unique id and IMEI number of GSM module, as two identities required, to implement MICA.

Following are the details of the join message format and data message format:

A. Join Message Format

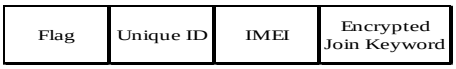

Fig. 1: Join Message Format

Following is the description of the fields of the join message format as shown in Fig. 1:

Flag value describes whether the message is a join message or a data message. Its value is '0' for join message.

Unique id is the identification number of ultrasonic sensor which is unique.

IMEI number is the unique identification numeric of GSM module.

Encrypted Join Keyword is used for verifying the authenticity of the join message where original join keyword is some fixed value e.g. "MICA"

B. Data Message Format

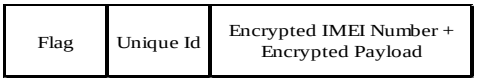

Fig. 2: Data Message Format

Following is the description of the fields of the data message format as shown in Fig. 2:

Flag value describes whether the message is a join message or a data message. Its value is '1' for join message.

Unique id is the identification number of ultrasonic sensor which is unique.

Encrypted IMEI number is the unique identification numeric of GSM module. It is half of the length and encrypted.

Encrypted Payload is the original message and it's encrypted.

The combination of encrypted IMEI number and encrypted payload is placed as one field in data message.

III. ENCRYPTION PROCESS

Both join message and data message are important entities in MICA. Disclosure of any one of them would lead to the breach of security. So the encryption of both the messages is mandatory. In MICA the encryption process of join message and data message is different as non-repudiation, data confidentiality, authentication and data integrity should be achieved.

A. Encryption Process of Join Message

Fig. 3 shows the encryption process of the join message wherein sensor's unique id alongside IMEI number of GSM module are the input for key generation. The generated key is used to encrypt the join key word. Finally encrypted join key word is generated.

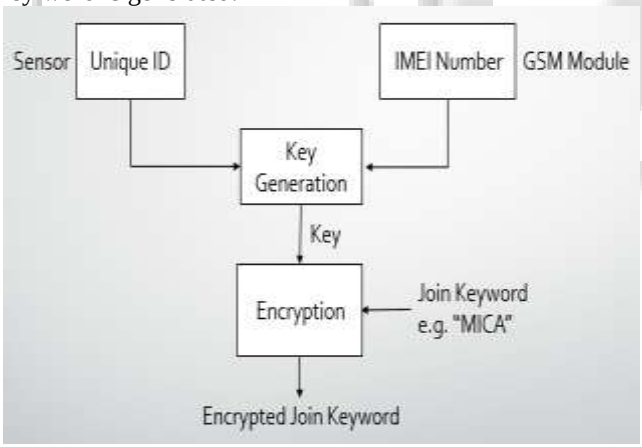

Fig. 3: Encryption Process of Join Message

B. Encryption Process of Data Message

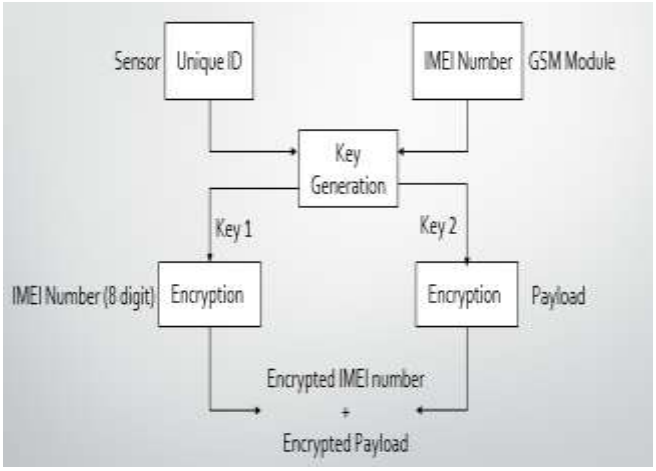

Fig. 4: Encryption Process of Data Message

Fig. 4 shows the encryption process of the data message wherein sensor's unique id alongside IMEI number of GSM module are the input for key generation. The key generation process here differs from that of join message encryption. Key generation logic generates two different keys and are used to encrypt two different things. One is the eight digit IMEI number of the GSM module and the second is payload. Encrypted payload then is merged with the encrypted IMEI number of the GSM module.

IV. DECRYPTION PROCESS

To retrieve the original join message or data message, decryption process takes place. Even decryption process is different for both join and data message. Below is the detail explanation of the decryption process.

A. Decryption Process at Server of Join Message

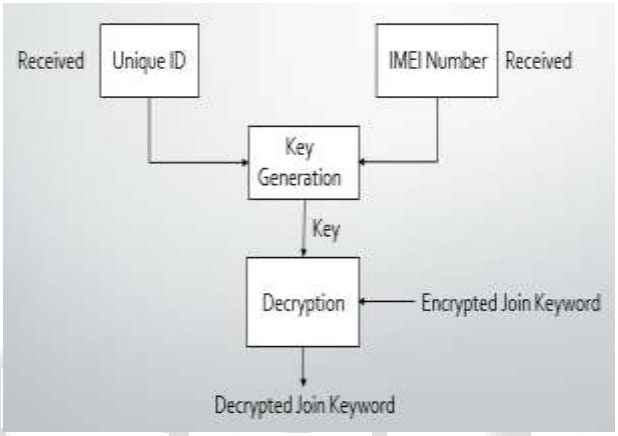

Fig. 5: Decryption Process at Server of Join Message

Fig. 5 shows the decryption process of the join message. For key generation, received unique id of sensor and IMEI number of GSM module are used. Encrypted join key word is decrypted by the generated key. It compares the decrypted join keyword with the original join keyword. If they match, it stores unique id of sensor and IMEI number of GSM module into the database else discard the join message.

B. Decryption Process at Server of Data Message

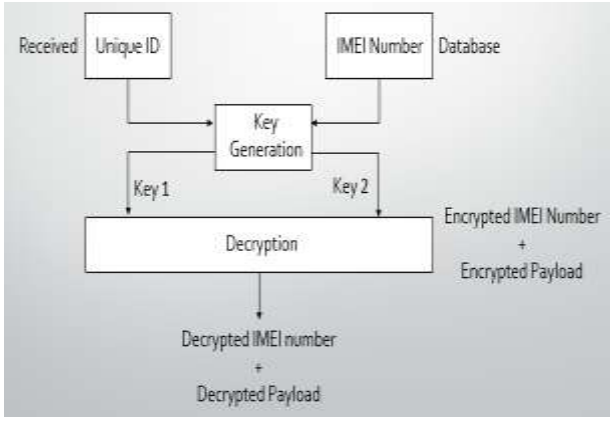

Fig. 6: Decryption Process at Server of Data Message

Fig. 6 shows the decryption process of the data message. For key generation, received unique id of sensor and IMEI number of GSM module from the database are used. Key generation in decryption process varies from that of join message. Here two keys are generated. Key-1 decrypts the encrypted IMEI number + encrypted payload and matched with original eight digit IMEI number. If it matches, the

same things are decrypted with Key-2, extract the original payload and then store it into the database.

So by splitting the process into two message format, we can achieve non-repudiation, data confidentiality, authentication and data integrity.

V. SIMULATION AND RESULTS

The comparison is performed with symmetric-key cryptography, asymmetric-key cryptography and multiple identity-based cryptography.

A. Performance Analysis of DES and RSA Cryptography

In a paper by Sombir, et al.[6] Symmetric key cryptography and Asymmetric key cryptography algorithms are explained with parameters like execution speed and its strength. In Symmetric key Cryptography, it takes DES and in Asymmetric key cryptography, it takes RSA as a consideration. As per paper, the experiment was performed on the machine [Intel® Pentium ® CPU G 630 @ 2.70 GHz, 2GB of RAM]. The operating system and system software used for these algorithms are Windows XP Service Pack 3.0 and Turbo C++ 3.0.

Here execution time of DES and RSA is in seconds. Table 1 represents the execution speed of this algorithm against the 5 different sizes of data.

1) Analysis:

This paper proves that encryption time of DES (Symmetric key algorithm) is always lesser than RSA (Asymmetric key algorithm). Hence we can say that Asymmetric algorithm execution speed is quite slower and also it require more resources for execution.

In our Scenario, algorithm will run on the small scale devices which have small processing power and less resources. So we cannot use Asymmetric algorithm in our scenario. Symmetric key algorithm provides the confidentially and integrity of data.

Input File Size (KB)	Encryption Execution Time(seconds)	
	DES	RSA
15	4.543859	5.63736
30	9.087718	11.27472
45	13.16158	16.91209
60	18.17544	23.54945
75	22.7193	29.18681

Table 1: DES and RSA Execution time for Encryption

B. Performance Analysis of AES, DES and MICA Cryptography

Symmetric key cryptography and Identity-based cryptography algorithms are compared below using parameters like execution speed and its strength. In Symmetric key Cryptography, it takes AES, DES and in Identity-based cryptography, it takes MICA as a consideration. The experiment was performed on the machine [Intel® Pentium ® CPU G 630 @ 2.70 GHz, 3GB of RAM]. The operating system and system software used for these algorithms are Windows 7 and Eclipse Luna.

Table 2 represents the execution speed of this algorithm against the 7 different sizes of data. Here execution time of AES, DES and MICA are in milliseconds.

Input File Size (KB)	Encryption Execution Time (milliseconds)		
	AES	DES	MICA
5	77.6	302.8	46.6
15	191	849.2	87.2
25	290.6	1393.6	115.4
35	375.2	1967.8	137.2
45	473	2429.4	168.8
55	574	2964.4	190.6
65	660.6	3551	196.8

Table 2: AES, DES sand MICA Execution time for Encryption

Fig. 7 shows the graphical representation of table 2.

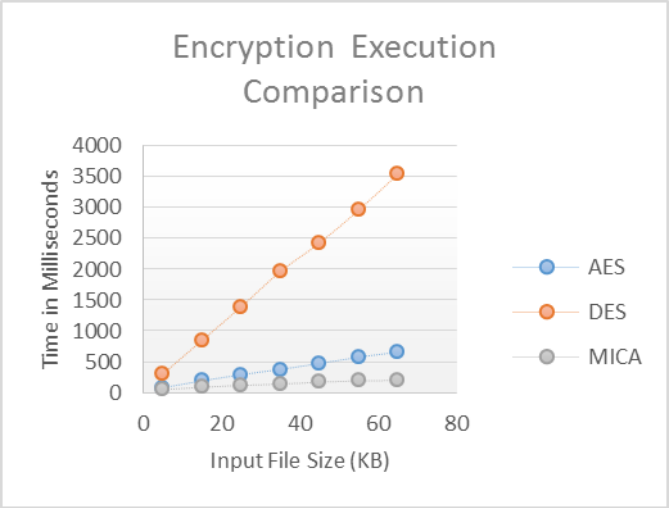

Fig. 7: Encryption Execution Comparison with AES, DES and MICA for small Input file sizes

Table 3 represents the execution speed of this algorithm against the 6 different sizes of data. Here execution time of AES, DES and MICA are in seconds.

Input File Size (MB)	Encryption Execution Time (seconds)		
	AES	DES	MICA
1	9.7116	54.8544	3.6052
2	19.085	106.2812	6.7268
3	27.9352	156.7156	10.1086
4	38.9496	208.4962	12.358
5	46.8262	259.6482	17.3926
6	52.4438	303.6548	19.4374

Table 3: AES, DES and MICA Execution time for Encryption

Fig. 8 shows the graphical representation of table 3.

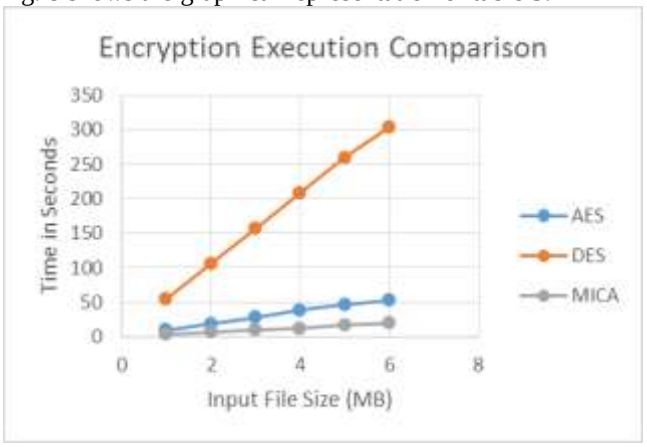

Fig. 8: Encryption Execution Comparison with AES, DES and MICA for large Input file sizes

C. Analysis:

Encryption time of AES, DES (Symmetric key algorithm) is always more than MICA. Hence we can conclude that AES, DES have quite slower execution speed and also require more resources compared to MICA. In our Scenario, where algorithm will be required to run on the small scale devices having small processing power and less resources, it is best to use multiple identity-based cryptography algorithm - MICA.

REFERENCES

[1] Coron, J.-S. "What is cryptography?", Security & Privacy, IEEE (Volume:4 , Issue: 1), Page(s):70 – 73
[2] Chandra, S., Paira, S., Alam, S.S., Sanyal, G. "A comparative survey of Symmetric and Asymmetric Key Cryptography", Electronics,Communication and Computational Engineering (ICECCE), 2014 International Conference on 17-18 Nov. 2014, page: 83 – 93
[3] Ritika Chehal, Kuldeep Singh "Efficiency and Security of Data with Symmetric Encryption Algorithms" Volume 2, Issue 8, August 2012
[4] Dr. Najib A. Kofahi "An Empirical Study to Compare the Performance of some Symmetric and Asymmetric Ciphers", International Journal of Security and Its Applications Vol.7, No.5 (2013), pp.1-16
[5] Comparison of Symmetric and Asymmetric Cryptography with Existing Vulnerabilities and Countermeasures-IJSAM JOURNAL
[6] Sombir Singh, Sunil K Maakar and Dr. Sudesh Kumar "A Performance Analysis of DES and RSA Cryptography" IJETTCS - Volume 2, Issue 3, May – June 2013

